



THE STOP & SHOP
COMPANIES, INC.

P.O. BOX 269, BOSTON, MA 02101
1 BRADLEES CIRCLE, BRAINTREE, MA 02184

MISSY GREALY
Director of Corporate Affairs
TEL (617) 380-8512

DOCKET FILE COPY ORIGINAL

93-292

~~STOP 1170~~

JAN 18 1994

TELECOPY COVER SHEET

TO:

He. William K. Calton

FROM:

MISSY GREALYGOVERNMENT AFFAIRS

DATE:

January 14, 1994

FAX #:

202-653-5402

RE:

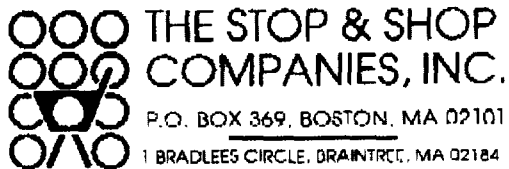
CC Docket No. 93-292PAGES
(inc. cover)9

IF YOU DID NOT RECEIVE ALL OF THE PAGES OR FIND THAT THEY
ARE ILLEGIBLE, PLEASE CALL JOSEPHINE SEVERINO AT

Telephone (617) 770-6023

Fax (617) 770-6013

No. of Copies rec'd
List ABCDE1 copy



DOCKET FILE COPY ORIGINAL

LAW DEPARTMENT

Peter M. Phillipps
VICE PRESIDENT
GENERAL COUNSEL and SECRETARY
TEL (617) 300-7005
FAX (617) 380-8309

January 14, 1993

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
Common Carrier Bureau
1919 M Street NW
Washington, DC 20554

Dear Mr. Caton:

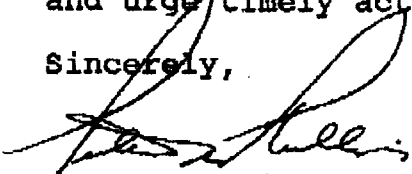
RE: Policies and Rules Concerning Toll Fraud, CC Docket No. 93-292,
Notice of Proposed Rulemaking (NPRM).

The following are the summary recommendations of The Stop & Shop Companies, Inc., with respect to the above-referenced proposed rulemaking:

- 1) The FCC should revise the current tariffs to permit a fair allocation of liability for toll fraud among equipment manufacturers, carriers and users.
- 2) Equipment manufacturers should be required to provide the disclosure and security information proposed by the FCC.
- 3) Carriers should be required to provide timely and effective warnings to users.

A description of the Company's experience with toll fraud, along with comments on specific provisions of the proposed rulemaking, are attached. We applaud the Commission's leadership in this area and urge timely action on this important business issue.

Sincerely,



Peter M. Phillipps

Attachments:

A. Comments on CC Docket No. 93-292

B. Testimony submitted to the Subcommittee on Telecommunications and Finance, House Committee on Energy and Commerce.

Attachment A.RE: CC Docket No. 93-292Comments of The Stop & Shop Companies, Inc.

III.

A. The following are comments in response to testimony given at the En Banc hearing and to FCC questions and proposals. Numbering follows the sequence of questions beginning on Page 7 of the Notice adopted November 10, 1993.

11. Current methods to battle toll fraud

It should be clarified that effective methods to battle toll fraud exist for known methods only.

While non-carrier insurance products to cover user exposure for telephone fraud exist, they are ineffective due to high price and limited coverage.

No proactive education programs are offered to our company by carriers.

16. Safeguards available to carriers

Carriers are in the best position to monitor traffic patterns and call volumes.

17. Forgiveness from liability

Forgiveness of charges should be available for at least three billing cycles to allow recapture of all total billing records (TBR) and thus identify full exposure prior to settlement of charges.

18. Customized call blocking

Customized call blocking should be extended to public, as well as private networks.

20. PBX capacity to install disabling features. / Non-card call screening

PBX operators lack sufficient knowledge to install disabling features. This knowledge resides with the equipment manufacturers, who do not develop the product with toll fraud in mind.

Carriers have the data in toll office billing switches with billing records to engage in screening and blocking functions for non calling card calls.

-page two-

21. Ability of carriers to distinguish legitimate PBX calls from fraudulent ones.

Carriers could distinguish legitimate PBX calls if the user identifies which calls should be blocked in the public network.

22. Outgoing calls on Incoming Lines.

PBX users do not have the capability to know whether call manager calls are outgoing calls originated on incoming lines.

23. Deregulation.

Deregulation did not contemplate technology and fraud developments that exist today. Given these developments, this is an appropriate arena for FCC regulation.

24. Current Tariff Liability Provisions.

We support the Commission's conclusions that tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of risks of using carrier services are unreasonable. We support the Commission's conclusion that carriers have an affirmative duty to ensure that these warnings are communicated effectively to customers through, for example, billing inserts, timely notice by account representatives and account teams, seminars, hands-on training and quarterly audits.

25. Proposed Liability Determinations

We support the approach suggested by the Commission with respect to apportionment of liability based upon determination of those who are in the best position to avoid, detect, warn of or control the fraud. We agree that specific responsibilities of carriers, equipment manufacturers and users should be defined, so that liability can be determined for failure to meet these responsibilities.

Damages for aggrieved parties should be in the form of relief of liability for charges for toll fraud.

Commission involvement, if necessary, should begin with alternative dispute resolution.

Attachment B.

Thursday June 11, 1992

Subcommittee on Telecommunications and Finance

Committee on Energy and Commerce

United States House of Representatives

Washington, D.C.

Written Testimony Submitted for the Record by The Stop & Shop
Companies, Inc.

Testimony of Stop & Shop on Telecommunications Fraud

I. Introduction

We are grateful to Chairman Markey for convening an oversight hearing on the issue of telecommunications fraud.

By way of establishing our credentials on the subject, we operate state-of-the-art telecommunications systems at over 250 locations. Our annual voice communications expenditures are approximately \$6 million. As one of the nation's leading retailers, with 1991 sales of \$5 billion and 42,000 employees, it is generally to our advantage to be on the cutting edge of an important issue. Unfortunately, in this case, we developed our considerable expertise in toll fraud out of necessity.

We have been the victim of toll fraud on three occasions over the past fourteen months. Our potential financial exposure from these incidents is over three hundred thousand dollars. Despite the expenditure of considerable time and resources to protect against further incidents, we consider ourselves still at risk.

Federal involvement is needed to clarify jurisdiction among enforcement agencies and to establish appropriate carrier responsibility. We urge the committee to use this hearing and the legislation filed by Congressman Frank (H.R. 5202) as the basis for developing an appropriate legislative remedy which will provide necessary protection to both public and private telecommunications users.

II. Background on three incidents of fraud over the past fourteen months.

In all three cases telephone hackers gained illegal access to our headquarters PBX (private branch exchange) via our 1-800 toll free DISA (Direct Inward System Access) trunks by compromising our DISA authorization code. Under normal conditions all DISA access to outbound service is restricted in the PBX software so that calls can only be made to internal extensions.

In two cases, once the hackers gained illegal access to our PBX, they utilized sophisticated computer software to take advantage of a temporary lapse in PBX calling privilege restrictions to obtain the access codes for our local and long distance lines and then place outbound calls. We believe that an error occurred during the performance of routine maintenance activities that changed or left access to our outbound services unrestricted.

Stop & Shop
Page Two

In the third case, once the hackers gained illegal access to our PBX, they utilized Call Manager, a standard feature of the AT&T network, to bypass the PBX software restrictions to our outbound services and place outbound calls.

III. Internal efforts to correct the fraud problem.

In response to these incidents of fraud, we have put in place a number of security measures aimed at preventing illegal use of our system in the future. These measures include:

- *installation of administrative software for switch maintenance.
- *installation of secured dial-back modems for remote access to PBX administrative ports.
- *implementation of specific restrictions to international countries that we do not do business with.
- *monitoring of the previous day's call activity through the implementation of a multi-part daily "call detail" review function.
- *testing of all our toll free numbers three times a day to insure that restrictions are in place.
- *daily testing to cover the latest known hacker techniques.
- *restrictions on credit card type calls (0+ dialing) from toll free DISA trunks.

Telephone security experts are completing an in-depth audit. The audit includes:

- *assessment of the vulnerability of our private branch exchanges.
- *assessment of the software restrictions put in place by our vendors.
- *security review of our future technology investment plans.

Based on the outcome of this audit, we anticipate expanding our security controls as follows:

- *implementation of increased employee training.
- *a written call restriction procedure with vendors.
- *a daily verification of security controls.

We also continue to work extensively with our new switch maintenance vendor as well as with security personnel from New England Telephone and AT&T. Through conferences, seminars and written materials, our professional staff attempts to stay current with new hacking methods and to identify new internal security procedures.

Despite our internal controls, hackers have continued their extensive efforts to gain access to our network. We are convinced that telephone fraud can and will happen to anyone. Resolution of the problem will require external, as well as internal action.

Stop & Shop
Page Three

IV. Assessment of current problems.

As noted above, current law is inadequate in two areas. First, the lines of responsibility for enforcement are unclear. Second, there is no carrier responsibility.

In the enforcement area, we have provided to the Secret Service all the available information relating to our three incidents of fraud. To date, we are not aware of any specific enforcement activity by that agency. We need aggressive enforcement by an agency with the high technology resources necessary to respond to high technology crime.

In addition, a central clearing house should be established for exchange of incident information and hacker methods, so that reactive security can be put in place. Finally, the current penalties are woefully inadequate and should be increased substantially. We hope that the committee will address these enforcement issues in developing legislation in this area.

While improvements in enforcement will help, the responsibility for preventing the problem must lie, in large part, with the carrier. Users will continue to be at risk until the carrier takes the steps necessary to outwit the hackers. Carriers can do this by updating their technology to correct faults in system design which result in network vulnerabilities.

Carriers also must commit to a high level of mutual assistance and cooperation with company users. Unfortunately, this has not been our experience. There was no discussion of security methods by the carrier when the system was installed. There was no response by the carrier to our request for assistance in defining access areas and remedies prior to the fraud. After our security was breached, our vendor kept us at arm's length or gave us non-responsive information, e.g., that security advisories are sent only to equipment customers, not network customers.

Finally, when the fraud is not the result of user negligence, users should not be responsible for the cost. Presently, we are not even limited to the true incremental cost of the fraud. Rather, the carrier stands to make a profit from our loss! This situation certainly provides no incentive to address the problem.

Stop & Shop
Page Four

V. Legislation introduced by Congressman Frank (H.R. 5202)

We applaud Congressman Frank for filing legislation establishing federal oversight in this area. The bill adopts an even-handed standard for assigning responsibility. It establishes carrier liability for toll charges, except in cases of customer negligence in the operation of equipment, or failure to provide timely notice. The rulemaking process required by the bill will yield helpful data on this issue for carriers, customers, regulators and this committee.

We urge this committee to use the Frank bill as a basis for developing more comprehensive legislation, including a strong enforcement process and protection for private customers.

VI. Conclusion

In conclusion, we would like to point out that high technology telecommunications crime and computer crime is as pervasive as the technology explosion itself. High technology crime is a critical issue. It will continue to undermine modern business and government operations until legislation is enacted to provide effective law enforcement and protection.

We would be pleased to provide additional information and technical expertise to assist in the development of a legislative solution to this problem. Thank you for the opportunity to participate in the hearing on this important issue.